Могилевский институт МВД

УДК 343.72:004.7

Т. С. Вайда
заведующий кафедрой специальной физической и огневой подготовки Херсонского факультета Одесского государственного университета внутренних дел, кандидат педагогических наук, доцент (Украина)

СКИММИНГ И ВИШИНГ КАК СОВРЕМЕННЫЕ ВИДЫ ИНТЕРНЕТ-МОШЕННИЧЕСТВА С БАНКОВСКИМИ ПЛАТЕЖНЫМИ КАРТОЧКАМИ В УКРАИНЕ

Интернет-мошенничество с банковскими карточками становится все более массовым явлением в Украине с тех пор, как ее граждане стали активно пользоваться пластиковыми платежными инструментами. Широкое использование населением электронных платежных карточек стало привлекать к себе внимание мошенников. В результате обмана граждане по различным причинам теряют значительные средства: 1) из-за собственной беспечности (храня, например, PIN-коды платежных карточек в кошельках); 2) становятся жертвами хорошо подготовленных правонарушителей-хакеров, которые узнают реквизиты банковских счетов граждан с помощью компьютерных вирусов, и т. д. Результат таких правонарушений с финансовыми ресурсами всегда один: человек остается без денежных средств.

В 2016 году 63 % всех краж в Украине приходилось на интернет-мошенничества с использованием платежных карточек. Еще 24 % краж совершали через банкоматы, 9 % — через системы интернет-банкинга и 4 % через POS-терминалы (эквайринговая сеть). По мнению О. Данильченко, такая тенденция сформировалась за последние два года — мошенники сосредоточили свое внимание именно на владельцах платежных карточек [1].

Социально-экономическая опасность поднятой нами проблемы подтверждается не только значительным увеличением количества краж денежных средств у владельцев платежных карточек, но и фиксацией правоохранителями новых схем афер. Стоит отметить, что уровень подготовленности грабителей постоянно растет, видоизменяется и методика совершения преступлений: приемы их атак на законопослушных граждан становятся все более утонченными.

Чаще всего пароли и данные карточек украинцев выманивают или через специально созданные сайты (фишинг), или способом личного общения мошенников с жертвой по телефону (вишинг). В первом случае используют внешний вид сайтов, предназначенных для перевода денег из одной карточки на другую (пополнения счета мобильных телефонов и т. п.). Как отмечают специалисты организации ЭМА, первый такой сайт в списке результатов поискового запроса будет фишинговым с вероятностью 98 %. За прошлый период количество таких ресурсов выросло в 4,5 раза: с 38 в 2015 году до 174 в 2016.

За 1–2 дня фишинговый сайт может «скомпрометировать» 800–2500 платежных карт [1].

Целью нашей работы является: 1) рассмотрение вишинга и скимминга как наиболее распространенных методов мошенничества, в которых правонарушителями для завладения денежными средствами владельцев используются реквизиты их банковских платежных карт; 2) предоставление рекомендаций собственникам таких карт для потенциальной минимизации случаев хищений денег.

Определение условий дальнейшего усовершенствования профилактики мошенничества как криминального преступления, разработка эффективных путей организации борьбы с этим негативным социально-экономическим явлением нашли свое отображение в научных исследованиях многих украинских ученых, которые рассматривали разные аспекты этой проблемы (А. В. Смаглюк, А. В. Кравченко, В. Р. Мойсик, А. А. Патик, Р. М. Крикливый, Ю. Л. Шуляк и др.).

Вместе с тем таким аспектам поднятой нами актуальной для современного общества проблемы, как: 1) предупреждение, прекращение и привлечение к ответственности лиц, которые осуществляют мошенничество с платежными карточками; 2) повышение эффективности профилактики вышеуказанного преступления в контексте роста уровня банковского сервиса, которым активно пользуются граждане для удобства и мобильности, учеными уделялось недостаточно внимания. Это позволяет конкретизировать цель нашего исследования и определить приоритетность задач.

Исследование проведено в соответствии с тематическим планом научно-исследовательской работы Одесского государственного университета внутренних дел по проблеме «Приоритетные направления развития и реформирования правоохранительных органов в условиях развертывания демократических процессов в государстве» (государственный регистрационный № 0116U006773).

В соответствии с Уголовным кодексом Украины (Раздел VI. Преступления против собственности, статья 190 «Мошенничество») мошенничество — это завладение чужим имуществом или приобретение права на имущество путем обмана или злоупотребления доверием [2]. Как показывает практика (отзывы граждан в Интернете, полицейская и судебная деятельность и т. п.) и подтверждают статистические данные, которые собраны и обобщены правоохранительными органами, все чаще для совершения этого вида преступлений используются мобильные телефоны и интернет-сети. Такие случаи мошенничества в последнее время получили значительное распространение. По данным Генеральной прокуратуры Украины, за 1 полугодие 2017 года количество лиц, которым сообщено о подозрении относительно совершения мошенничества (статья 190 УК Украины), составляет 2386 граждан [3], из них наибольшее количество преступлений совершено лицами в возрасте от 18 до 28 лет (686 лиц). За аналогичный период 2016 года таких правонарушений, а соответственно и количество лиц, которым было сообщено о подозрении, бы-

ло выявлено 1694 [3], из них наибольше количество преступлений лицами совершенно в возрасте от 18 до 28 лет (639 лиц). За последние два года количество мошенничеств с помощью телефона и интернета выросло на 23 %.

Рассмотрим особенности некоторых видов мошенничеств, которые применяются для кражи средств с помощью платежных банковских карт.

1. Скимминг. Название этого вида мошенничества произошло от названия устройства — «скиммер» (с англ. skimmer, to skim — 1) снимать; 2) едва касаться, скользить по чему-либо; 3) быстро прочитать) — специальное техническое устройство, которое считывает реквизиты с магнитных полос банковских карт [4, с. 655]. С их помощью мошенники похищают данные платежных карточек. Скиммеры изготавливаются отдельно под каждый вид банкомата: как правило, они устанавливаются в паре с миниатюрной видеокамерой, которая может быть вмонтирована в накладную панель, которая крепится на банкомате, или же с накладной клавиатурой. Основное задание камеры или накладной клавиатуры — узнать PIN-код. После получения информации с магнитной полосы изготавливается поддельная платежная карточка, так называемый белый пластик (от цвета карточки), которую мошенники впоследствии используют для получения денежных средств в банкоматах. Для расчетов в магазинах изготовляется карточка с графическим дизайном, чтобы кассир не смог определить ее поддельность [5].

Основная рекомендация банковских работников гражданам, чтобы они не стали жертвой скиммеров, проверка тщательным образом банкомата еще до момента введения в него платежной карточки, в частности, на наличие накладной клавиатуры. Целесообразно обратить внимание на заставку монитора банкомата с информационным сообщением о его стандартном внешнем изображении (она должна совпадать с реальным видом автомата). Но даже после этого эксперты советуют всегда прикрывать рукой или портмоне клавиатуру банкомата при наборе PIN-кода — на случай, если в него вмонтирована видеокамера, которая может записать последовательность набора пользователем своего PIN-кода. Тогда мошенники не смогут воспользоваться информацией, даже если им удастся получить данные карточки. Те же методы защиты эксперты советуют использовать при вводе PIN-кода с использованием POS-терминалов.

2. Вишинг (с англ. vishing, с англ. voice — «голос»; fishing — «рыбалка») — это разновидность фишинга, сущность которого заключается в использовании автонабирателей вместе с интернет-телефонией (VoIP) для кражи конфиденциальных данных (пароли доступа, номера банковских карт и т. д.) [4, с. 274, 781]. Как вид интернет-мошенничества это преступление появилось в Украине в июле 2006 года, сейчас телефонные мошеннические действия составляют до 20 % всех случаев интернет-преступлений [1].

У этого мошеннического способа есть несколько разновидностей:

1. Клиенты платежной системы получают по электронной почте сообщение якобы от администрации или службы безопасности банка с просьбой уточнить свой счет, пароль и т. п. после «недавних хакерских атак». Но если

при фишинге ссылка в сообщении направляет собственника карточки на поддельный сайт, где и происходит кража информации, то в случае вишинга предлагается набрать определенный номер телефона. Далее лицу — потенциальной жертве, которому позвонили по телефону, зачитывается текст сообщения с просьбой предоставить свои конфиденциальные данные.

Популярная разновидность этой схемы интернет-мошенничества — рассылка SMS-сообщений с информацией о том, что платежная карточка жертвы заблокирована («Ваша карточка заблокирована»). В этом же SMS-сообщении указаны номера телефонов, куда можно позвонить и узнать все подробности. Доверчивые люди звонят по телефону на указанные номера мошенников, которые представляются работниками банка, и в ходе разговора преступники выясняют всю необходимую информацию о банковской карточке (PIN-код и т. д.).

Порой мошенники действуют более изобретательно: сообщают человеку о получении наследства или выигрыша в фейковой лотерее и уточняют реквизиты банковской карточки для перевода этих денег. В последние годы преступники стали намного изобретательнее, чем раньше (например, просят перечислить денежную сумму для уплаты налога за выигранный автомобиль).

2. Электронная почта вообще не используется: преступники программируют компьютер для выборочного набора телефонных номеров из длинного списка телефонного справочника, а лицо, которое отвечает на этот звонок, только прослушивает записанное сообщение. В сообщении предупреждается, что информация о платежной карточке ее собственника попала к мошенникам, и в связи с этим просят ввести с клавиатуры мобильного телефона номер карты для блокирования.

Применение протокола VoIP помогает снизить учреждениям расходы на телефонную связь, но вместе с тем делает их интернет-сети более уязвимыми для хакерских нападений. Банки и другие организации, которые используют для голосовой связи IP-телефонию, рискуют быть подверженными вишинг-атакам, для профилактики которых пока нет надежных средств.

3. Обычный обман владельца платежной карточки по телефону: мошенник выдает себя за работника службы безопасности банка или его call-центра и, ссылаясь на сбой в компьютерной системе (оперативно выявленную попытку кражи денежных средств) и потерю некоторых данных, просит клиента (умело поддерживая у него возникшую растерянность из-за потери собственных средств или проявляя беспокойство об их сохранности) назвать все реквизиты его карточного счета — точные личностные данные (Ф.И.О., год рождения, номер карточки, срок ее действия, коды безопасности, когда последний раз пользовались карточкой, состояние баланса денежных средств, какие были последние транзакции, сумма перевода и т. п.).

Вишингом занимаются лица даже из мест лишения свободы (граждане, осужденные за мошенничество и имеющие доступ к мобильному телефону): они звонят людям и, используя приемы психического давления, вынуждают перечислить деньги на свой карточный счет якобы за освобождение их детей

при задержании полицией, для оперативного оказания медпомощи члену семьи после аварии и т. д.

4. С помощью SMS-сообщений о выигрыше в несуществующей лотерее (акции) мошенники стимулируют (непринужденно заставляют) владельца карточки звонить по телефону и предоставлять свои реквизиты для перечисления денежных средств.

5. Мошенники «сами хотят приобрести товар» у продавца, предлагают перечислить денежные средства этому лицу на его карточный счет, узнавая таким образом у жертвы персональные данные (номер карточного счета и т. д.). После этого мошенники звонят по телефону «из банка» и от имени «банковского работника» сообщают продавцу о поступлении средств, которые готовы перевести на его счет. Для правильного завершения банковской операции предлагают получателю средств срочно (например, в конце банковского дня, перед выходными, в обеденный перерыв и т. д.) подойти к ближайшему банкомату. Дальше под диктовку псевдоработника банка человек нажимает цифры и таким образом переводит деньги на другой счет (т. е. люди сами отдают свои деньги). Понять, что это мошенник, можно сразу же после того, как у собственника карточки попросят назвать PIN-код и код безопасности платежной карточки, которые указаны на ее обратной стороне (CVV2/CVC2 используется при осуществлении покупок в Интернете). Оба кода — это конфиденциальная информация, которую ни в коем случае нельзя сообщать ни работникам банка, ни третьим лицам. Настоящий банковский работник никогда не запрашивает таких данных.

Как свидетельствуют результаты опроса владельцев платежных карт, проведенного агентством Gemius в Украине, 77 % жителей знают, что нельзя предоставлять реквизиты карточки, кроме ее номера, но 76 % все-таки раскрывают эти данные в стрессовой ситуации [1].

Эти же данные могут быть затребованы аферистами и по электронной почте — в виде письма от банка. Как правило, его текст составляется так, что у человека нет сомнений в истинности уведомления от банка, в котором он обслуживается (иначе откуда менеджеру знать дату открытия счета). Аферисты часто покупают информацию о клиентах у нечистых на руку работников банка.

С целью избежания воровства денежных средств с карточного счета владельцам платежной карточки ни при каких условиях не сообщать ее данные третьим лицам. Если это по какой-то причине все-таки случилось, то сразу же необходимо сообщить об этом в финансово-кредитную организацию, заблокировать банковский счет, а потом заменить карточку.

Мошенники пытаются и другими способами узнать побольше частной информации, которая будет необходима для прохождения идентификации в call-центре банка. Если им это удается, то преступники поднимают лимит снятия наличности и получают значительно больше денег, чем при обычном вишинге.

Собственнику банковской карточки нужно сравнивать телефонный номер банка (указан на карточке, банкомате) с теми номерами, которые присылаются в SMS-сообщении: если номера не совпадают, значит, это SMS-сообщение от аферистов. Чтобы убедиться в этом, лицу надо позвонить по телефону в банк и уточнить все обстоятельства.

Благодаря методам социальной инженерии (специальные приемы общения) преступники вынуждают разглашать личные данные или платить мошенникам средства за определенные вымышленные услуги, например, оплата эвакуатора (или вынужденного ремонта на СТО) для выигранного в акции автомобиля, поломка которого (техническая неисправность) произошла по пути к своему счастливому владельцу.

Профилактика данного вида преступления (мошенничества с платежными карточками) заключается прежде всего в осведомленности граждан о существующих современных схемах, которые применяются преступниками с использованием методов социальной инженерии.

Для улучшения информированности населения об интернет-мошенничествах целесообразно объединить усилия правоохранительных органов, банковских учреждений, средств массовой информации и т. п.

Самим гражданам необходимо критически относиться к информации, которую они получают через мобильные телефоны, интернет-сети и т. д., оперативно проверять ее в банковских учреждениях и своевременно блокировать банковский счет.

Список основных источников

1. Карточные мошенники научились по-новому воровать деньги в украинцев [Электронный ресурс]. – Режим доступа: http://intemetua.com/kartocsnie-moshenniki-naucsilis-po-novomu-vorovat-dengi-u-ukraincev. – Дата доступа: 11.01.2018.

2. Уголовный кодекс Украины [Элекронный ресурс] : Закон Украины, 5 апр. 2001 г., № 2341-III. – Режим доступа: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341 -14. – Дата доступа: 11.01.2018.

3. Единый отчет о лицах, которые совершили криминальные правонарушения за январь–июнь 2017 года [Электронный ресурс]. – Режим доступа: http://www.gp.gov.ua/ua/stst2011.html?dir id=113277&libid=100820&c=e dit& c=fo#. – Дата доступа: 11.01.2018.

4. Мюллер, В. К. Англо-русский словарь : 53 000 слов / В. К. Мюллер. – 21-е изд., испр. – М. : Рус. яз., 1987. – С. 655.

5. Лысенко, Е. Шесть приемов против карточных мошенников в Украине [Электронный ресурс] / Е. Лысенко. – Режим доступа: http://vesti.ua/poleznoe/23667-kak-ukraincam-uberech-bankovskie-karty-ot-moshennikov. – Дата доступа: 11.01.2018.